IN THE UNITED STATES OF DISTRICT COURT
FOR THE EASTERN DISTRICT OF NORTH CAROLINA
WESTERN DIVISION
NO. 5:09-CR-216-8

UNITED STATES OF AMERICA,	)	
Plaintiff	)	DEFENDANT YAGHI'S
	)	MEMORANDUM OF LAW
v.	)	IN SUPPORT OF MOTION
	)	TO SUPPRESS FISA
ZIYAD YAGHI,	)	DERIVED EVIDENCE
Defendant	)	

Defendant Ziyad Yaghi, through counsel, submits this Memorandum of Law in Support of Motion to Suppress FISA Derived Evidence.

STATEMENT OF THE FACTS

Yaghi was indicted on or about July 22, 2009 alleging in Count One conspiracy to provide material support to terrorists, as defined in 18 U.S.C. § 2339A; and Count Two conspiracy to murder, kidnap, maim and injure persons as defined in 18 U.S.C. § 956(a). The Indictment has been Superseded twice (First Superceding on September 24, 2009 and the Second Superseding Indictment on November 24, 2010).

On 27 July 2009, the Government filed a "Notice of Intent to Use Foreign Intelligence Surveillance Act Information" as to Yaghi. (D.E. 40). The Notice states that the Government "intends to offer into evidence or otherwise use or disclose in any proceedings in the above-captioned matter, information obtained and derived from electronic surveillance and physical search conducted pursuant to [FISA]." *Id.*

The Government has not confirmed any details about what evidence derived from FISA searches and surveillance will be used in the prosecution of this case. However, based on the voluminous discovery materials provided, including both general discovery and "sensitive but

unclassified" ("SBU") materials, Yaghi believes the FISA Derived Evidence includes at a minimum electronic surveillance; telephone wiretaps; computer and phone searches; and residence searches. Upon information and belief, most, if not all, of the surveillance occurred within the United States, Jordan and Egypt.

Yaghi, a naturalized citizen, has been detained since his arrest on the charges in the Indictment.

ARGUMENT

I. STANDARD OF REVIEW.

This Court reviews the FISA applications and Foreign Intelligence Surveillance Court's ("FISC") orders *de novo*. *See, e.g., United States v. Hammoud*, 381 F.3d 316, 332 (4th Cir. 2004) (noting district court's *de novo* review and conducting its own *de novo* review of FISA materials), *vacated on other grounds*, 543 U.S. 1097 (2005); *United States v. Squillacote*, 221 F.3d 542, 554 (4th Cir. 2000) (same).

A reviewing court essentially conducts the same review of the FISA application and associated materials that the FISC judge initially conducted upon receiving an application requesting an order under FISA. *See In re Grand Jury Proceedings of Special April 2002 Grand Jury*, 347 F.3d 197, 204-05 (7th Cir. 2003); *United States v. Mubayyid*, 521 F. Supp. 2d 125, 131 (D. Mass. 2007). The Court reviews, first, the adequacy of the FISA materials at issue "de novo with no deference accorded to the FISC's probable cause determinations," and second, the executive branch's certifications, which are reviewed for clear error. *See, e.g., United States v. Rosen*, 447 F. Supp. 2d 538, 545 (E.D. Va. 2006).

There are important reasons for engaging in *de novo* review of FISA materials. *In camera, ex parte* review was triggered by the Government's submission of the Attorney

General's affidavit. *See* 50 U.S.C. §§ 1806(f), 1825(g). Under these circumstances, *de novo* review is necessary because the reviewing court's consideration of the FISA materials is "unaided by the adversarial process." *See United States v. Rosen*, 447 F. Supp. 2d at 545 (rejecting Government's contention that FISC's probable cause determination should be accorded "substantial deference"); *United States v. Warsame*, 547 F. Supp. 2d 982, 990 (D. Minn. 2008) (same).

The FISA process is exceptionally one-sided in nature. *See United States v.Warsame*, 547 F. Supp. 2d at 987. Unless and until the Court grants Yaghic's Motion for Disclosure of FISA Applications and Orders, Yaghi is barred from articulating the opposing view because he does not have access to that information. The Court, therefore, must function as a stand-in for defense counsel with respect to the assessment of these FISA materials. Upon review, the Government has the opportunity to argue that the facts contained in the affidavit are sufficient to support probable cause.

Finally, courts repeatedly cite the presence of a judicial intermediary as an essential reason why FISA passes constitutional muster. *See, e.g. United States v. Cavanagh*, 807 F.2d 787, 791 (9th Cir. 1987); *United States v. Duggan*, 743 F.2d 59, 73-74 (2d Cir 1984); *United States v. Belfield*, 692 F.2d 141, 148 (D.C. Cir. 1982). This judicial intermediary is, in the first instance, the FISC judge and the probable cause assessment the judge must make. In the context of this prosecution, this Court serves an essential function as such an intermediary as well.

II. FISA VIOLATES THE FOURTH AMENDMENT.

The Fourth Amendment's warrant requirement limits the power of the Government to conduct investigations against the citizenry. Fourth Amendment jurisprudence has refined the warrant requirement and the core concepts that give meaning to this important constitutional

protection -- concepts such as probable cause, the detached magistrate, notice and particularity. Prior to the adoption of the Patriot Act, a line of Circuit Court cases, including the Fourth Circuit's seminal decision in *United States v. Truong Dinh Hung*, 629 F.2d 908 (4th Cir. 1980), recognized that the traditional Fourth Amendment warrant requirements may be relaxed where the primary purpose of an investigation is for foreign intelligence purposes.

In October 2001, through the Patriot Act, Congress amended FISA, changing the language that "the purpose" of the search or surveillance was to obtain foreign intelligence information, to "a significant purpose." *See* 50 U.S.C §§ 1804(a)(7)(B), 1823(a)(7)(B). This change in FISA's language enables the Government to gather evidence for a criminal prosecution without the protections afforded by the Fourth Amendment. FISA, as amended, is unconstitutional on its face. The courts have recognized that the Fourth Amendment's reasonableness requirement must be considered in the context of a national security investigation, but FISA now goes too far and impermissibly undercuts the Fourth Amendment's protections.

A. The Supreme Court's Electronic Surveillance Cases.

The Supreme Court first applied the Fourth Amendment to electronic surveillance in *Katz v. United States*, 389 U.S. 347 (1967), and *Berger v. New York*, 388 U.S. 41 (1967). *Katz* involved the surreptitious recording of telephone calls through a recording device attached to the outside of a telephone booth. The *Katz* Court declared that "[t]he Government's activities in electronically listening to and recording the petitioner's words violated the privacy upon which he justifiably relied while using the telephone booth and thus constituted a 'search and seizure' within the meaning of the Fourth Amendment." 389 U.S. at 353. The Court held that the warrantless surveillance violated the Fourth Amendment, in part because the Government agents

failed, "before commencing the search, to present their estimate of probable cause for detached scrutiny by a neutral magistrate." *Id*. at 356. The Supreme Court rejected the Government's request for a "telephone booth" exception to the warrant requirement. *Id*. at 358. It expressly left open, however, "[w]hether safeguards other than prior authorization by a magistrate would satisfy the Fourth Amendment in a situation involving the national security." *Id.* at 358 n.23.

In *Berger*, which arose from electronic surveillance conducted by state law enforcement officers, the Court emphasized that the traditional probable cause and particularity requirements apply to warrants or other orders authorizing such surveillance. *See* 388 U.S. at 55-56. The Court found that the New York statute authorizing the surveillance violated the Fourth Amendment (1) because it did not "requir[e] belief that any particular offense has been or is being committed; nor that the 'property' sought, the conversations, be particularly described"; (2) because it failed to limit the duration of the surveillance or to impose sufficiently stringent requirements on renewals of the authorization; and (3) because the statute "has no requirement for notice as do conventional warrants, nor does it overcome this defect by requiring some showing of special facts." *Id.* at 58-60. *Berger* rejected the state's argument that Fourth Amendment requirements should be relaxed because the surveillance statute was essential in its fight against organized crime. In terms that ring as true today as they did when it issued the *Berger* opinion, the Court declared:

> [W]e cannot forgive the requirements of the Fourth Amendment in the name of law enforcement. This is no formality that we require today but a fundamental rule that has long been recognized as basic to the privacy of every home in America. . . . Few threats to liberty exist which are greater than that posed by the use of eavesdropping devices.

Id. at 62-63 (quotation and citation omitted); *see, e.g., Mincey v. Arizona*, 437 U.S. 385, 393 (1978) ("[T]he mere fact that law enforcement may be made more efficient can never by itself

justify disregard of the Fourth Amendment. . . . The investigation of crime would always be simplified if warrants were unnecessary. But the Fourth Amendment reflects the view of those who wrote the Bill of Rights that the privacy of a person's home and property may not be totally sacrificed in the name of maximum simplicity in enforcement of the criminal law.").

The Supreme Court addressed the question left open in *Katz* – the limits that the Fourth Amendment places on electronic surveillance conducted in the name of national security – in *United States v. United States District Court (Keith)*, 407 U.S. 297 (1972). *Keith* considered the constitutional limits on surveillance directed at domestic security threats; the Court noted that the case "requires no judgment on the scope of the President's surveillance power with respect to the activities of foreign powers, within or without this country." *Id.* at 308; *see id.* at 321-22 ("We have not addressed, and express no opinion as to, the issues which may be involved with respect to activities of foreign powers or their agents."). Although the Court recognized both the weight of the executive's interest in protecting the national security and the value of electronic surveillance in detecting security threats, it found that "[t]here is, understandably, a deep-seated uneasiness and apprehension that this [surveillance] capability will be used to intrude upon cherished privacy of law-abiding citizens. We look to the Bill of Rights to safeguard this privacy." *Id.* at 312-13 (footnote omitted). The Court emphasized the need to protect both First and Fourth Amendment rights against

government investigation based on alleged threats to national security:

> History abundantly documents the tendency of Government – however benevolent and benign its motives – to view with suspicion those who most fervently dispute its policies. Fourth Amendment protections become the more necessary when the targets of official surveillance may be those suspected of unorthodoxy in their political beliefs. The danger to political dissent is acute where the Government attempts to act under so vague a concept as "domestic

> security." Given the difficulty of defining the domestic security interest, the danger of abuse in acting to protect that interest becomes apparent.

Id. at 314. The Court emphasized the importance of the Fourth Amendment warrant requirement in protecting the right of privacy. It identified as "the very heart of the Fourth Amendment directive" that

> where practical, a governmental search and seizure should represent both the efforts of the officer to gather evidence of wrongful acts and the judgment of the magistrate that the collected evidence is sufficient to justify invasion of a citizen's private premises or conversation. Inherent in the concept of a warrant is its issuance by a "neutral and detached magistrate." The further requirement of "probable cause" instructs the magistrate that baseless searches shall not proceed.

Id. at 316 (citations omitted). And the Court made clear that the decision to conduct electronic surveillance cannot be left to the discretion of law enforcement officials:

> These Fourth Amendment freedoms cannot properly be guaranteed if domestic security surveillances may be conducted solely within the discretion of the Executive Branch. . . . [T]hose charged with this investigative and prosecutorial duty should not be the sole judges of when to utilize constitutionally sensitive means in pursuing their tasks. The historical judgment, which the Fourth Amendment accepts, is that unreviewed executive discretion may yield too readily to pressures to obtain incriminating evidence and overlook potential invasions of privacy and protected speech.

Id. at 316-17 (citation and footnote omitted). The Court rejected the Government's argument that an exception to the Fourth Amendment warrant requirement should be recognized for domestic security surveillance. In particular, the Court did not find persuasive the Government's claims that "internal security matters are too subtle and complex for judicial evaluation" and that "prior judicial approval will fracture the secrecy essential to official intelligence gathering." *Id.* at 320.

Finally, *Keith* underscored the differences between surveillance for criminal investigative purposes and surveillance for intelligence purposes. It noted, for example, that "[t]he gathering of security intelligence is often long range and involves the interrelation of various sources and types of information"; that "[t]he exact targets of such surveillance may be more difficult to

identify than in surveillance operations against many types of crime specified in Title III"; and that "[o]ften, too, the emphasis of domestic intelligence gathering is on the prevention of unlawful activity or the enhancement of the Government's preparedness for some possible future crisis or emergency." *Id.* at 322. In light of these "potential distinctions between Title III criminal surveillances and those involving the domestic security," the Court suggested that Congress "may wish to consider protective standards for the latter which differ from those already prescribed for specified crimes in Title III," *id.* – a suggestion that led ultimately to the enactment of FISA in 1979. The Court added that "[d]ifferent standards may be compatible with the Fourth Amendment if they are reasonable both in relation to the legitimate need of Government for intelligence information and the protected rights of our citizens." *Id.* at 322-23 (emphasis added).

B. Surveillance And Searches For The Primary Purpose Of Obtaining Foreign Intelligence Information.

Read together, *Katz*, *Berger*, and *Keith* draw a line between surveillance conducted by law enforcement officials for the purpose of investigating crime – which requires the traditional warrant based on probable cause, as outlined in *Berger* and codified in 18 U.S.C. § 2518 – and surveillance conducted by intelligence officials for the purpose of obtaining intelligence information. Probable cause would appear to be associated with a prosecution and intelligence to prevention. Herein we are concerned with prosecution.

Until the Patriot Act, both Title III and FISA clearly recognized this constitutionally-mandated distinction. And in the years following *Keith* – before and after the enactment of FISA – courts relied on the Supreme Court's distinction between "criminal surveillances" and surveillance conducted for intelligence purposes to hold that

electronic surveillance may proceed without the protections of a traditional warrant based on probable cause only if a court determines that the primary purpose of the surveillance is to obtain foreign intelligence information. *See United States v. Truong Dinh Hung*, 629 F.2d 908, 915-16 (4th Cir. 1980) ("[T]he executive should be excused from securing a warrant only when the surveillance is conducted 'primarily' for foreign intelligence reasons."); *see also, e.g., United States v. Johnson*, 952 F.2d 565, 572 (1st Cir. 1991) ("Although evidence obtained under FISA subsequently may be used in criminal prosecutions . . . the investigation of criminal activity cannot be the primary purpose of the surveillance. [FISA] is not to be used as an end-run around the Fourth Amendment's prohibition of warrantless searches."); *United States v. Butenko*, 494 F.2d 593, 606 (3d Cir. 1974) (en banc) ("Since the primary purpose of these searches is to secure foreign intelligence information, a judge, when reviewing a particular search must, above all, be assured that this was in fact its primary purpose and that the accumulation of evidence of criminal activity was incidental."); *United States v. Bin Laden*, 126 F. Supp. 2d 264, 277-78 (S.D.N.Y. 2000) (foreign intelligence exception to warrant requirement for searches abroad where, among other requirements, search is "conducted 'primarily' for foreign intelligence purposes"); *United States v. Megahey*, 553 F. Supp. 1180, 1188-89 (E.D.N.Y. 1982) (foreign intelligence exception to warrant requirement applies when surveillance is conducted "primarily" for foreign intelligence reasons), *aff'd sub nom. United States v. Duggan*, 743 F.2d 59 (2d Cir. 1984).

The *Truong Dinh Hung* court, and cases that followed it, mandated that the *primary purpose* of the investigation is to gather foreign intelligence information and not to gather evidence to mount a criminal prosecution, because "once surveillance becomes primarily a criminal investigation, the courts are entirely competent to make the usual probable cause

determination, and because, importantly, individual privacy interests come to the fore and government foreign policy concerns recede when the government is primarily attempting to form the basis for criminal prosecution." 629 F.2d at 915. The Fourth Circuit has not questioned its analysis in *Truong Dinh Hung*, and it remains the law in this Circuit. This review becomes more apparent in the prosecution context when combines with rights related to both speech and religion.

C. FISA Is Facially Unconstitutional.

The fundamental problem with FISA, as amended by the Patriot Act, is that the Government now is empowered to conduct searches and electronic surveillance under FISA's relaxed standards and secret procedures even if the Government's primary purpose is to gather evidence of domestic criminal activity. The differences between FISA procedures and traditional search warrant or Title III electronic surveillance procedures are substantial. These differences include the following.

First, FISA orders approving electronic surveillance or searches may be obtained without a showing of probable cause, as Fourth Amendment jurisprudence has traditionally defined that concept. Probable cause under the Fourth Amendment is probable cause to believe that a crime has been or is about to be committed. Under FISA, however, an order may be obtained authorizing electronic surveillance or a search merely upon a showing of probable cause to believe that the target of the order is "a foreign power or an agent of a foreign power" and that the facilities or places to be surveilled or searched are being used or are about to be used by a foreign power or an agent of a foreign power. *See* 50 U.S.C. §§ 1805(a)(3), 1825(a)(3). In *Berger v. New York*, as discussed above, the Supreme Court struck down a state eavesdropping statute in part because it did not require a probable cause showing that a particular crime had been or was

being committed. 388 U.S. at 58-60. The relative ease of obtaining a FISA order as opposed to a traditional search warrant or a Title III electronic surveillance order is amply illustrated by what apparently transpired in this case. There does not appear to be any evidence that the Yaghi (or any of the other defendants) was the agent of a foreign power, yet whatever evidence the Government presented apparently was deemed sufficient for the Government to invoke the FISA mechanisms and obtain orders authorizing the electronic interceptions and physical seizures.

Second, FISA does not require notice to the target that a search or that electronic surveillance has occurred. By contrast, the Fourth Amendment generally requires that the subject of a search be notified that the search has taken place. *See, e.g.*, *Wilson v. Arkansas*, 514 U.S. 927, 930 (1995) (holding that common-law "knock-and-announce" principle forms part of the Fourth Amendment reasonableness inquiry). The Fourth Amendment also generally requires that the target of electronic surveillance be given timely notice that the surveillance has occurred. *See, e.g.*, *Berger v. New York*, 388 U.S. at 60 (holding that state statute authorizing electronic surveillance violated Fourth Amendment in part because it contained no requirement that notice be given to target.) Under FISA, notice is never given to the target unless a criminal prosecution ensues.

Third, the FISA secrecy provisions are unconstitutional. When notice is given to a defendant that a FISA search or that electronic surveillance has occurred, the notice which the statute requires is constitutionally insufficient. Under FISA, when the Government intends to use FISA derived evidence at a hearing or at trial, the statute requires only that the Government give notice of such intent. *See* 50 U.S.C. §§ 1806(c) and 1825(d). The Government provided that minimal notice in this case. FISA does not require that a copy of the FISC order be provided or that the FISC application papers be revealed. This level of secrecy with respect to the

Government's authority to conduct a search or electronic surveillance is inconsistent with the Fourth Amendment because it unreasonably handicaps the ability of the target of the search or surveillance to challenge the legality of the government action. *Cf.* 18 U.S.C. § 2518 (9) (requiring service of copy of court order and accompanying application under which wire, oral or electronic interception is authorized.) When motions to suppress are filed under FISA, the Government is allowed to submit *ex parte* papers to the Court which the Court then uses to determine the motion. Yaghi has requested disclosure of the FISA applications and orders in a related motion.

Fourth, FISA procedures violate the particularity requirement of the Fourth Amendment. FISA orders authorizing searches or electronic surveillance may issue upon a finding by the FISC judge that there is probable cause to believe that the target of the order is a foreign power or the agent of a foreign power and that the facilities to be surveilled and places to be searched are being used or are about to be used by a foreign power or an agent of a foreign power. FISA suffers from the same constitutional frailties as the statute that was struck down in *Berger*. FISA orders are issued "without requiring belief that any particular offense has been or is being committed; nor that the 'property' sought, the conversations, be particularly described. The purpose of the probable-cause requirement of the *Fourth Amendment,* to keep the state out of constitutionally protected areas until it has reason to believe that a specific crime has been or is being committed, is thereby wholly aborted. Likewise, the statute's failure to describe with particularity the conversations sought gives the officer a roving commission to 'seize' any and all conversations." 388 U.S. at 58-59. Although FISA orders are issued after a certification by the officer applicant that the information sought is deemed to be "foreign intelligence information,"

that broad categorization of information does not satisfy the constitutional requirement that the property or conversations sought be particularly described.

Fifth, FISA procedures do not satisfy the constitutional requirement that warrants issue only after review by a "neutral and detached" magistrate. In passing on a FISA application, the FISC judge is required to accept the certifications of the officer applicant unless those certifications are "clearly erroneous." *See* 50 U.S.C. §§1805(a)(5) and 1824(a)(5). Rather than being "neutral and detached," the FISC judge is constrained by the statutory provisions and may not independently review the application papers. Furthermore, there is no requirement in FISA that the Government agents make any return to the court regarding the items seized or the conversations recorded. *Cf.* Fed. R. Crim. P. 41(f); 18 U.S.C. § 2518(8)(a).

Finally, the duration of FISA orders is unconstitutionally long. FISA surveillance against a U.S. person like Yaghi may be for a term up to 90 days without any further judicial oversight. In *Berger*, the Supreme Court expressed concern about the duration of intercept orders where the statute authorized a term of up to two months. 388 U.S. at 59. By contrast, Title III, which was drafted with the *Berger* constitutional constraints in mind, authorizes interceptions for only 30 days at a time. *See* 18 U.S.C. § 2518 (5).

For all these reasons, FISA's "blanket grant of permission to eavesdrop is without adequate judicial supervision or protective measures." *Berger*, 388 U.S. at 60. *See generally Mayfield v. United States*, 504 F. Supp. 2d 1023 (D. Or. 2007) (holding FISA unconstitutional), *vacated and remanded on other grounds*, 599 F.3d 964 (9th Cir. 2009) (plaintiff lacked standing).

III. YAGHI IS ENTITLED TO AN ORDER SUPPRESSING THE FISA DERIVED EVIDENCE.

If the Court determines that FISA passes constitutional muster, it will then determine the lawfulness of the surveillance authorized under FISA. The Court reviews the probable cause determination, the executive branch certifications, and the conduct of the subsequent surveillance. If the Court determines that the electronic surveillance or physical search "was not lawfully authorized or conducted, it shall . . . suppress the evidence which was unlawfully obtained or derived from the electronic surveillance of the aggrieved person." 50 U.S.C. § 1806(g); *see id.* § 1825(h) (physical search).

Even if the evidence is not suppressed, the Court must disclose FISA materials to the defense if "due process requires discovery or disclosure" of the materials it examines. *Id.* §§ 1806(g), 1825(h). Additionally, if the Court cannot make an accurate determination of the legality of the surveillance or search, the Court "may disclose to the aggrieved person, under appropriate security procedures and protective orders, portions of the application, order, or other materials relating to the surveillance only where such disclosure is necessary to make an accurate determination of the legality of the surveillance." *Id.* §§ 1806(f) (electronic surveillance), 1825(g) (physical search).

A number of factors may bring the legality of FISA-authorized searches into question. Disclosure and an adversary hearing are appropriate where the Court's initial review of the application, order, and fruits of the surveillance or search:

> indicates that the question of legality may be complicated by factors such as indications of possible misrepresentations of fact, vague identifications of the persons to be surveilled, or surveillance records which include a significant amount of nonforeign intelligence information, calling into question compliance with the minimization standards contained in the order.

United States v. Belfield, 692 F.2d 141, 147 (D.C. Cir. 1982) (internal quotation and footnote omitted).

Reviewing courts should be "mindful of possible biases when [] assess[ing] the adequacy of the government's allegations," since the officials charged with overseeing such operations have a professional interest in their success. *See United States v. Ott*, 827 F.2d 473, 476 (9th Cir. 1987). Because of the one-sided nature of the *ex parte* review of FISA materials, **the reviewing court functions as the only guardian of a criminal defendant's constitutional and statutory rights**.

FISA was designed with foreign intelligence information in mind, and "a significant purpose" of FISA surveillance and searches must be "to obtain foreign intelligence information." 50 U.S.C. §§ 1804(a)(6)(B), 1823(a)(6)(B). Although the statute contemplates that the information so collected may be used in the criminal justice context, *id*. §§ 1806(d), 1825(d), the foreign policy purpose of the surveillance should be plainly apparent. *See United States v. Belfield*, 692 F.2d at 147.

In this case, Yaghi is limited in his ability to challenge the FISA applications and orders, and the conduct of the subsequent surveillance, because he has been barred access to those materials. Yaghi has filed a related motion seeking disclosure of those materials. In the next sections of this brief, Yaghi outlines the grounds he believes may be available to suppress the evidence under FISA.

A. The FISA Derived Evidence Is Subject To Suppression Because The Information Sought Was Not Foreign Intelligence Information, And Obtaining Foreign Intelligence Information Could Not Have Been A Significant Purpose.

FISA defines "foreign intelligence information" as:

> (1) information that relates to, and if concerning a United States person is necessary to, the ability of the United States to protect against –
>
> > (A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;

> (B) sabotage, international terrorism, or the international proliferation of weapons of mass destruction by a foreign power or by an agent of a foreign power; or
>
> (C) clandestine intelligence gathering activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or
>
> (2) information with respect to a foreign power or foreign territory that relates to, and if concerning a United States citizen, is necessary to –
>
> (A) the national defense or security of the United States; or
>
> (B) the conduct of the foreign affairs of the United States.

50 U.S.C. § 1801(e).

In the voluminous discovery produced by the Government, including hundreds of hours of audio and video recordings, computer files, and records and other materials seized in physical searches, there is a complete absence of any evidence suggesting that Yaghi or any of the other defendants was involved in activities that could justify a determination that the information sought was necessary to protect the United States against actual or potential attack, sabotage, international terrorism, the international proliferation of weapons of mass destruction, or clandestine intelligence gathering activities.

As discussed above, Yaghi has challenged the constitutionality of FISA's requirement that the Government must show only that obtaining foreign intelligence information is a "significant purpose." Although the Patriot Act amendments diluted the primary purpose test to the lesser standard of "significant purpose," a purpose-based standard still exists. The FISA Court of Review addressed this issue as follows.

> Similarly, FISA surveillance would not be authorized against a target engaged in purely domestic terrorism because the government would not be able to show that the target is acting for or on behalf of a foreign power. As should be clear from

> the foregoing, FISA applies only to certain carefully delineated, and particularly serious, foreign threats to national security.

In re Sealed Case, 310 F.3d 717, 739 (FISA Ct. Rev. 2002). The FISA derived evidence was unlawfully acquired and is properly suppressed.

B. The FISA Derived Evidence Is Subject To Suppression Because There Was No Probable Cause To Believe Yaghi Was An "Agent Of A Foreign Power."

The probable cause assessment is the core substantive judicial determination that a FISC judge must make in authorizing foreign intelligence surveillance under FISA. *See* 50 U.S.C. §§ 1805(a), 1825(a). The FISC judge's probable cause assessment **is not** entitled to deference. *See, e.g, Warsame*, 547 F. Supp. 2d at 990; Rosen, 447 F. Supp. 2d at 545. FISA specifies that:

> [i]n determining whether or not probable cause exists . . . a judge may consider past activities of the target, as well as facts and circumstances relating to current or future activities of the target.

50 U.S.C. §§ 1805(b), 1825(b).

The substantive standard for probable cause is specific to FISA. *See, e.g. Warsame*, 547 F. Supp. 2d at 992-94. Instead of directing a judge or magistrate to find probable cause to believe that a crime was committed, a FISC judge must find that there is probable cause to believe that the target is a foreign power or agent of a foreign power, and that the facilities or locations sought to be searched are being used by a foreign power or agent of a foreign power. *See id*.; 50 U.S.C. § 1805(a)(2). A FISC judge may enter an order approving an electronic surveillance under FISA only if the court concludes that:

> on the basis of the facts submitted by the applicant there is pobable cause to believe that –
>
> (A) the target of the electronic surveillance is a foreign power or an agent of a foreign power: *Provided*, that no United States person may be considered a

> foreign power or an agent of a foreign power solely upon the basis of activities protected by the first amendment of the Constitution of the United States; and
>
> (B) each of the facilities or places at which the electronic surveillance is being directed is being used, or is about to be used, by a foreign power or an agent of a foreign power.

50 U.S.C. § 1805(a)(2).

The same probable cause finding is also required for physical searches, except that the judge must find that "the premises or property to be searched is or is about to be owned, used, possessed by, or is in transit to or from an agent of a foreign power or a foreign power." *See id.* § 1824(a)(2).

"Agent of a foreign power," in turn, means any United States person who:

> (A) knowingly engages in clandestine intelligence gathering activities for or on behalf of a foreign power, which activities involve or may involve a violation of the criminal statutes of the United States; [or]
>
> (B) pursuant to the direction of an intelligence service or network of a foreign power, knowingly engages in any other clandestine intelligence activities for or on behalf of such foreign power, which activities involve or are about to involve a violation of the criminal statutes of the United States;
>
> (C) knowingly engages in sabotage or international terrorism, or activities that are in preparation therefor, for or on behalf of a foreign power;
>
> (D) knowingly enters the United States under a false or fraudulent identity for or on behalf of a foreign power or, while in the United States, knowingly assumes a false and fraudulent identity for or on behalf of a foreign power; or
>
> (E) knowingly aids or abets any person in the conduct of activities described in subparagraph (A), (B), or (C), or knowingly conspires with any person to engage in activities described in subparagraph (A), (B), or (C).

Id. §§ 1801(b)(2), 1821(1).

Yaghi cannot be sure what basis the Government invoked to support a probable cause finding that he was an "agent of a foreign power." It is noteworthy that the voluminous discovery

produced by the Government, after its use of FISA authorized searches and seizures, reveals no evidence of clandestine intelligence gathering, international terrorism, or use of false or fraudulent identities.

Because it is the most indefinite, Yaghi believes it is most likely that the Government attempted to show that Yaghi (and likely the other defendants subjected to FISA searches and seizures) knowingly engaged in acts in preparation for international terrorism for or on behalf of a foreign power. *Id.* § 1801(b)(2)(C). Yaghi further believes it is likely that the Government attempted to establish the necessary involvement of a "foreign power" by attempting to show Yaghi's (and the other defendants') involvement with "a group engaged in international terrorism or activities in preparation therefor." *Id.* § 1801(a)(4). However, there is no evidence, even after the FISA-authorized searches and seizures, of planned acts of international terrorism, or any involvement with a group engaged in international terrorism.[1] Yaghi contends that where the Government's allegations of overt acts in the Indictment, and the evidence of the Government's searches and seizures, show a unified focus on protected First Amendment speech, association, and religious activities, the probable cause finding was improperly based on such First Amendment activities. *See* 50 U.S.C.

---

[1] "International terrorism" means activities that –

(1) involve violent acts or acts dangerous to human life that are a violation of the criminal laws of the United States or of any State, or that would be a criminal violation if committed within the jurisdiction of the United States or any State;

(2) appear to be intended–

(A) to intimidate or coerce a civilian population;
(B) to influence the policy of a government by intimidation or coercion; or
(C) to affect the conduct of a government by assassination or kidnapping; and

> (3) occur totally outside the United States or transcend national boundaries in terms of the means by which they are accomplished, the persons they appear intended to coerce or intimidate, or the locale in which their perpetrators operate or seek asylum.

50 U.S.C. § 1801(c).

§ 1805(a)(2)(A).

Since the definition of "agent of a foreign power" probably involved here requires engaging in activities that involve, may involve, or will involve a violation of a criminal statute, this Court examines each application to ensure that it specifies the criminal statutes that are or are likely to be violated. Then, the Court must decide whether the application materials include sufficient facts to justify the belief that the target has engaged in behavior that violates those statutes.

C. The FISA Derived Evidence Is Subject To Suppression Because The Government Did Not Establish The Other Necessary Statutory Prerequisites.

Apart from the probable cause assessment, the Court was required to review each application to ensure that it meets the additional standards set out by FISA. Here, this Court's authority to review the certifications of the executive branch is no greater than the FISC court's authority. *See, e.g. United States v. Campa*, 529 F.3d 980, 993 (11th Cir. 2008). However, because this Court examines FISA materials *de novo*, no deference is accorded to the FISC judge's assessment of the executive branch certifications.

First, the court must find that: (1) the application was made by a Federal officer, (2) the application was approved by the Attorney General, and (3) the proposed minimization procedures meet the statutory definitions of minimization contained in 50 U.S.C. § 1805(a) for electronic surveillance, and § 1821(4) for physical searches. *See id.* §§ 1805(a), 1824(a). The electronic surveillance evidence produced by the Government is consistent with an indiscriminate plan of electronic surveillance rather than one follows proper minimization

procedures. *See United States v. Belfield*, 692 F.2d at 147 ("surveillance records which include a significant amount of nonforeign intelligence information, calling into question compliance with the minimization standards contained in the order").

Second, the court must find that the application contains the statements and certifications required by statute, and that those statements and certifications were made by a designated official. *Id.* §§ 1805(a)(4), 1824(a)(4). The following statements and certifications must accompany any application for an order approving searches and surveillance under FISA:

- A statement of the proposed minimization procedures;

- A statement of the nature of the foreign intelligence information sought and the type of communications or activities to be subjected to the surveillance, or the manner in which the physical search is to be conducted;

- Certifications by an authorized official that:

  the certifying official deems the information sought to be foreign intelligence information; a significant purpose of the search is to obtain foreign intelligence information;

  that such information cannot reasonably be obtained by normal investigative techniques; and

- A statement explaining the basis for the certifications above.

50 U.S.C. §§ 1804(a), 1823(a). Since Yaghi is a United States person, the court must assess these statements and executive branch certifications to determine that they are not "clearly erroneous." *Id.* §§ 1805(a)(4), 1824(a)(4). A "clearly erroneous" finding is established when "although there is evidence to support it, the reviewing court on the entire evidence is left with the definite and firm conviction that a mistake has been committed." *See United States v. United States Gypsum Co.*, 333 U.S. 364, 395 (1948). As argued above, the absence of evidence that could have supported the Government's claim that it was seeking "foreign intelligence information,"

through surveillance of an "agent of a foreign power," who was engaged in acts of, or preparation for "international terrorism," compels the conclusion that the Government's certifications were clearly erroneous.

The judicial oversight in this arena can fairly be characterized as minimal, insofar as neither the FISC judge nor this Court is to "second-guess" the certifications of the executive branch. *See, e.g. United States v. Duggan*, 743 F.2d at 77. However, the existence of a judicial check on the assertions of the executive branch in the FISA context is vital to FISA's legality. This Court will not rubber stamp on the executive's certifications.

Investigations involving FISA searches and surveillance are different in kind from ordinary criminal investigations: "FISA is meant to take into account the differences between ordinary criminal investigations to gather evidence of specific crimes and foreign counterintelligence investigations to uncover and monitor clandestine activities." *United States v. Sarkissian*, 841 F.2d 959, 965 (9th Cir. 1988) (citation and quotation omitted). The Government did not honor this distinction, and as a result, the FISA derived evidence is properly suppressed.

CONCLUSION

For the foregoing reasons, defendant Ziyad Yaghi respectfully requests that the Court issue an appropriate order suppressing all FISA Derived Evidence and granting such other and further relief as the Court deems just and proper.

This the 24th day of February, 2011.

/s/ James M. Ayers II
Attorney for Defendant Ziyad Yaghi
Ayers & Haidt, P.A.
307 Metcalf Street
Post Office Box 1544
New Bern, North Carolina 28563
Telephone: (252) 638-2955
Facsimile: (252) 638-3293
jimayers2@embarqmail.com
State Bar No. 18085
Criminal – Appointed

CERTIFICATE OF SERVICE

I hereby certify that a true and correct copy of the foregoing ***DEFENDANT YAGHI'S MEMORANDUM OF LAW IN SUPPORT OF MOTION TO SUPPRESS FISA DERIVED EVIDENCE*** was filed with the clerk of court for the Eastern District of North Carolina using the electronic filing system of the court. The electronic case filing system sent a "Notice of Electronic Filing" to the following attorney of record:

Barbara D. Kocher, Esq.
Assistant U.S. Attorney
John S. Bowler, Esq.
Assistant U.S. Attorney
Jason Harris Cowley
Assistant U.S. Attorney
Suite 800, Federal Building
310 New Bern Avenue
Raleigh, NC 27601-1461

Debra Carroll Graves
Assistant Federal Public Defender
Rosemary Godwin
Assistant Federal Public Defender
Federal Public Defender's Office
150 Fayetteville Street, Suite 400
Raleigh, North Carolina 27601
Attorneys for Daniel Boyd

Jason M. Kellhofer
US Department of Justice
950 Pennsylvania Avenue NW
Room 2720
Washington, DC 20530

Robert J. McAfee
McAfee Law, P.A.
P.O. Box 905
New Bern NC 28563
rjm@mcafee-law.com
Attorney for Sherifi

Paul K. Sun
Ellis & Winters
Post Office Box 33550
Raleigh, North Carolina 27636
Attorney for Subasic

Myron T. Hill, Jr.
200 E. Fourth Street
P. O. Box 859
Greenville, NC 27835-0859
mhill@browning-hill.com
Attorney for Zakariya Boyd

Joseph E. Zeszotarski, Jr.
Poyner Spruill LLP
P.O. Box 1801
Raleigh, NC 27602
jzeszotarski@poyners.com
Attorney for Dylan Boyd

R. Daniel Boyce
Boyce & Boyce, PLLC
P.O. Box 1990
Raleigh, NC 27602-1990
dboyce@boyceandboyce.com
Attorney for Mohammad Hassan

This the 24th day of February, 2011.

/s/ James M. Ayers II
Attorney for Defendant Ziyad Yaghi
Ayers & Haidt, P.A.
307 Metcalf Street
Post Office Box 1544
New Bern, North Carolina 28563
Telephone: (252) 638-2955
Facsimile: (252) 638-3293
jimayers2@embarqmail.com
State Bar No. 18085
Criminal – Appointed